REMARKS

Claims 1-63 are pending. Claim 1 stands objected to as having an informality. Claims 1-63 stand rejected under 35 U.S.C § 102(e) as being anticipated by U.S. Patent No. 5,457,747 to Drexler et al.

Reconsideration is requested. No new matter is added. The rejections are traversed. Claims 1, 4, 5, 7, 32, 36, 37, and 39 are amended. Claims 64-67 are added. Claims 1-67 remain in the case for consideration.

Support for new claims 66-67 can be found in the paragraph beginning on page 43, line 1 of the specification.

REJECTION UNDER 35 U.S.C. § 102(e)

Referring to claim 1, the invention is directed toward a method for tokenless biometric authorization. At least one communication is formed. A user electronically submits a registration biometric sample. The registration biometric sample is electronically transmitted via a public communications network. The registration biometric sample is then stored in a master electronic identicator. The user then submits a bid biometric sample, which is transmitted to an electronic identicator. The user is identified by comparing the bid biometric sample with a registration biometric sample. Upon successful identification, an electronic communication is authorized. The entire method can be carried out without using smartcards or magnetic stripe cards.

Referring to claim 32, the invention is directed toward a system for tokenless biometric authorization. The system includes a communication input apparatus, which includes a data entry device to form an electronic communication. A biometric input apparatus includes a device to scan a biometric sample from the user. A master electronic identicator includes a database to store biometric samples from registered users and a comparator to compare received biometric samples with previously stored biometric samples. The system also includes a public network to transmit data between the biometric input apparatus and the master electronic identicator and an electronic communication authorization to authorize execution of a communication upon successful identification of the user. The system can operate without using smartcards or magnetic stripe cards.

In contrast, Drexler teaches a system for deterring fraudulent use of cards. The user has a card, which stores both the user's biometric sample and limits on the user of the card to obtain benefits. The user initially records his biometric sample on the card. Then, when the

user presents the card to obtain services, the user provides another biometric sample, which is compared with the biometric data stored on the card. If the biometric sample matches the biometric data stored on the card, then the user limit data is accessed from the card, and if the use requested by the person is authorized, the user receives the desired benefits.

The most obvious difference is that Drexler requires a card, whereas the invention does not. The use of the card is stated numerous times in Drexler: see Abstract, lines 1, 4, and 10-12; column 2, lines 31-32, and 54; column 3, lines 51-52; column 4, lines 12-13, and 35-36; and column 5, lines 33-35 for a smattering of references. In addition, as stated in column 3, lines 24-26, an advantage of Drexler is that it permits the use of the currently-installed base of magnetic stripe card readers: they can read the information needed to perform the anti-fraud measures of Drexler without replacing such equipment.

In contrast, claims 1 and 32 of the invention emphasize the tokenless nature of the invention: the word "tokenless" appears in the preamble to the claims, and the claims describe the method and system operating "without the user having to present smartcards or magnetic stripe cards." Since the very first thing the user has to do in Drexler is present the card (so that the biometric sample can be compared with that on the card), Drexler cannot anticipate a tokenless biometric system or method.

There are other differences as well between Drexler and the invention. The invention stores the registration biometric samples in a master electronic identicator, which includes a database of registration biometric samples from many users. Unless many people share the card of Drexler (a totally impractical idea), it will only store the biometric data for one person. Therefore, the Drexler card cannot be a database storing registration biometric samples from many users.

And if the Drexler card stores only one user's biometric data, Drexler cannot perform user *identification*. Identification is the process of determining a user's identity. In effect, identification answers the question "Who am I?" Identification assumes that there is no information already suggesting the user's identity. In contrast, *verification* answers the question "Am I who I say I am?" Because there is only one user's biometric data stored on the Drexler card, the user has already identified himself, and is asking the system to *verify his identity*.

Another way to look at the difference between identification and verification is to consider what happens in the equipment performing the processes. In identification, the offered biometric sample is compared with at least a subset of the registered biometric samples, so that the system can say, "Of all the registered biometric samples I looked at, the

offered biometric sample most likely matches this one." But in verification, the offered biometric sample is compared with *only one* registered biometric sample: the one associated with the person the user claims to be. The system says either "He is whom he says he is," or "He is not whom he says he is." The system makes no effort to compare the offered biometric sample with any other registered biometric sample to determine the user's true identity.

To give yet another explanation of the difference between identification and verification, consider the situation where a person is attempting to commit fraud and assert that he is someone else. (Note that avoiding fraud is the stated purpose of Drexler, both in the title and technical field of Drexler.) Drexler would compare the offered biometric sample of the criminal with that of the card, and determine that they do not match. Drexler would then deny the criminal the benefits he sought. In contrast, the invention would identify the criminal (assuming the criminal has registered with the system). This means that the police could be sent to arrest the criminal knowing his identity. Drexler cannot accomplish this, because Drexler does not perform identification.

Drexler mentions a library, which stores biometric information. But, as described at column 8, lines 7-27, Drexler uses the library only to re-verify the user's identity as an anti-fraud measure, and not for identification.

Finally, Drexler does not teach transmission, either of the registration biometric sample or of the bid biometric sample. In Drexler, the registration biometric sample is stored on the card, which is in the user's possession at the time of registration. And both the registered biometric sample and the offered biometric sample are locally available in Drexler when the user requests benefits. Drexler can compare the offered biometric sample with the biometric data stored on the card at the machine at the time the user makes the request for benefits: no transmission anywhere is needed. In contrast, in the invention the registration biometric sample is stored in the master electronic identicator. The master electronic identicator is typically remote (and secure) relative to the user's location, and therefore the registration biometric sample is transmitted from the place where it is received to the master electronic identicator. Similarly, the place where the user offers the bid biometric sample is typically remote from where the system performs identification of the user, and so the bid biometric sample is transmitted to the electronic identicator.

The invention as defined by claim 1 is directed toward:

A method for *tokenless biometric authorization* of an electronic communication, using a biometric sample, a master electronic identicator, and a public communications network, wherein said method comprises:

a. an electronic communication formation step, wherein at least one communication comprising electronic data is formed;

b. a user registration step, wherein a user electronically submits a registration biometric sample taken directly from a person of the user;

c. *a public network data transmittal step, wherein the registration biometric sample is electronically transmitted to a master electronic identicator via a public communications network, said master electronic identicator comprising a computer database which electronically stores all of the registration biometric samples from all of the registered users*;

d. a user registration biometric storage step, wherein the registration biometric sample is electronically stored within the master electronic identicator;

e. *a bid biometric transmittal step, wherein a bid biometric sample, taken directly from the person of the user, is electronically transmitted to at least one electronic identicator*;

f. *a user identification step, wherein an electronic identicator compares the bid biometric sample to at least one registration biometric sample previously stored in an electronic identicator, for producing either a successful or failed identification of the user*;

g. an electronic communication authorization step, wherein upon a successful identification of the user by an electronic identicator, at least one electronic communication is authorized for execution;

wherein an electronic communication is biometrically-authorized *without the user having to present smartcards or magnetic stripe cards.*

(claim 1; italics added). As these features are not taught or suggested by Drexler, claim 1 is patentable under 35 U.S.C. § 102(e) over Drexler. Accordingly, claims 1-31, 64, and 66 are allowable.

The invention as defined by claim 32 is directed toward:

A system for *tokenless biometric authorization* of an electronic communication, using an electronic communication input apparatus, a biometric input apparatus, and a master electronic identicator, wherein said system comprises:

a. a communication input apparatus, further comprising a data entry device for formation of an electronic communication;

b. a biometric input apparatus, further comprising a device for electronically scanning a biometric sample directly from a person of a user;

c. *at least one master electronic identicator*, further comprising:

i) *a computer database containing all of the electronically stored biometric samples from all of the registered users*;

ii) a comparator that electronically compares received a biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user;

d. *a data transmittal public network that electronically transmits data between the biometric input apparatus and a master electronic identicator*;

e. an electronic communication authorization platform that authorizes execution of at least one electronic communication upon a successful identification of the user by an electronic identicator;

wherein an electronic communication is biometrically-authorized *without the user having to present smartcards or magnetic stripe cards.*

(claim 32; italics added). As these features are not taught or suggested by Drexler, claim 32 is patentable under 35 U.S.C. § 102(e) over Drexler. Accordingly, claims 32-63, 65, and 67 are allowable.

Referring to claims 2-31 and 33-63, the Examiner did not present a prima facie argument that the inventions are anticipated by Drexler. The Examiner simply stated that these claims disclose the same inventive concepts as in claims 1 and 32. While claims 2-31 and 33-67 further define the inventions of claims 1 and 32, respectively, they also add further limitations that distinguish claims 2-31 and 33-67 over claims 1 and 32, and therefore are not the same inventive concepts. As the Examiner did not indicate where the limitations of claims 2-31 and 33-67 are specifically taught within Drexler, claims 2-31 and 33-67 should therefore be allowable with claims 1 and 32. Moreover, these claims add further inventive features that are patentable in their own right over Drexler: e.g., the rule-module of claims 17 and 49, and the use of a personal identification code in claims 66-67.

For the foregoing reasons, reconsideration and allowance of claims 1-63 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM
1030 SW Morrison Street
Portland, OR 97205
(503) 222-3613
Customer No. 20575

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Washington, DC 20231
Date: August 11, 2003

Ariel S. Rogson